METHOD AND APPARATUS FOR FACILITATING SECURE ANONYMOUS EMAIL RECIPIENTS

ABSTRACT

One embodiment of the present invention provides a system that facilitates secure transmission of an email message to anonymous recipients without divulging the identities of the anonymous recipients. This system constructs an email message by identifying recipients of the email message. These recipients can include known recipients, who can be identified by examining the email message, and anonymous recipients, who cannot be identified by examining the email message. The system also generates a session key for the email message, and encrypts a body of the email message with the session key. The system also creates a recipient block for the email message that contains an entry for each recipient of the email message. Each entry in this recipient block contains the session key encrypted with a public key associated with the recipient to form an encrypted session key, so that only a corresponding private key held by the recipient can be used to decrypt the encrypted session key. Each entry additionally contains an identifier for the associated public key, so that each recipient can determine whether the recipient possesses a corresponding private key that can decrypt the encrypted session key. These identifiers are constructed so that identifiers for public keys belonging to known recipients are statistically unique, and identifiers for public keys belonging to anonymous recipients are not statistically unique. Finally, the system sends the email message to the recipients.